(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－25051

(43)公開日　平成11年(1999)１月29日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ
1/00	３７０	1/00	３７０Ｅ

審査請求　未請求　請求項の数10　ＯＬ（全９頁）

(21)出願番号　特願平9－183433

(22)出願日　平成９年(1997)７月９日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　横沢　達
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

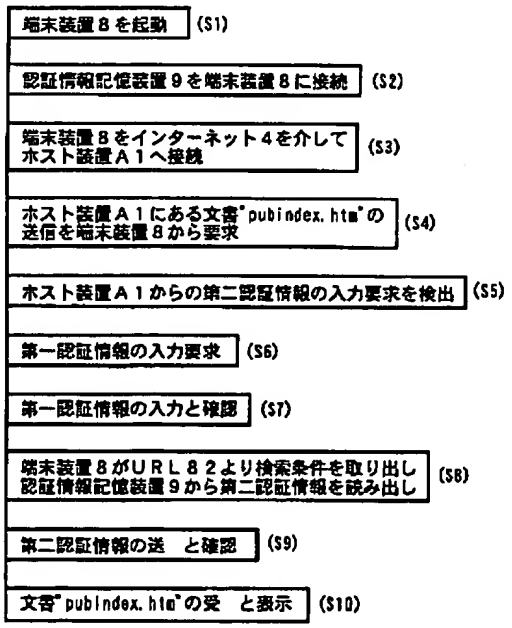
(72)発明者　安達　誠
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　情報システム

(57)【要約】
【課題】端末装置を複数箇所のホスト装置に接続するときに、複数の異なる認証情報が必要になる場合が有り、これでは利用者は必要な認証情報をすべて覚えている必要があり非常に煩わしい。
【解決手段】端末装置にホスト装置へ送信する複数の認証情報を記憶し、またこの認証情報を読み出す為にこれらとは別の認証情報を必要とし、またこの別に用意した認証情報を確認するための機能を備えた情報システム。

図　6



【特許請求の範囲】

【請求項１】各種情報を蓄積し、該情報を端末装置により利用者が取り出し可能で、該利用者が前記情報の取り出しを行うときに、利用者が正規の登録者であることを確認するための認証情報を利用者に要求する機能を有するホスト装置と、
該ホスト装置と接続してデータの送受信が可能で、前記各種情報を取り込み、これを利用者に提示する機能と、利用者からの入力を受ける機能を有する前記端末装置と、
からなる情報システムにおいて、
各種のデータを記憶し、前記端末装置によって該データの読書きをすることが可能で、かつ、該データの読書きする前に、これを許可するための第一認証情報を記憶し、さらに該許可処理を行う機能を有する認証情報記憶装置を備え、
該認証情報記憶装置が前記ホスト装置で必要となる認証情報を第二認証情報として記憶し、さらに該第二認証情報を選択的に読み書きできる機能を前記認証方法記憶装置または前記端末装置に備え、
第二認証情報を複数種類必要とする場合でも、利用者がそれぞれの認証情報を覚えなくとも、唯一前記第一認証情報だけを覚えるだけで簡単な選択で必要な第二認証情報を読み出して、前記ホスト装置への接続に必要な確認処理を完了できるようにしたことを特徴とする情報システム。

【請求項２】請求項１において、前記ホスト装置と前記端末装置がプロトコルによって情報の送受信を行う機能を備え、
前記端末装置が該プロトコルによって前記ホスト装置との接続に確認処理が必要であることを検出する機能と、該検出結果を契機として該端末装置が前記第二認証情報を前記認証情報記憶装置より読み出して前記ホスト装置へ送信する機能、および予め前記認証情報記憶装置への前記第一認証情報による確認手続きを完了しておく機能を備え、
前記ホスト装置より前記第二認証情報を要求されたときに、その度に利用者が前記第一認証情報の入力を行う必要がないようにしたことを特徴とする情報システム。

【請求項３】請求項２において、ホスト装置と端末装置がＴＣＰ／ＩＰによって接続され、前記第二認証情報を前記認証情報記憶装置から選択的に読み出すための条件情報として、ＩＰアドレスを用いることを特徴とする情報システム。

【請求項４】請求項１または請求項２において、前記第二認証情報を認証情報記憶装置から選択的に読み出すための条件情報が、ＵＲＬ（Uniform Resource Locator）を用いることを特徴とする情報システム。

【請求項５】請求項２において、予め第一認証情報によって行った前記認証情報記憶装置への読み書きが出来る有効な期間が、前記端末装置と前記ホスト装置との接続を切断する時に終了することを特徴とする情報システム。

【請求項６】請求項２において、予め第一認証情報によって行った前記認証情報記憶装置への読み書きが出来る有効な期間が、前記端末装置または認証情報記憶装置に予め設定された期間を経過すると終了することを特徴とする情報システム。

【請求項７】請求項２において、前記端末装置が予め設定された時間で自動的に端末機能を停止する機能を備える場合、予め第一認証情報によって行った前記認証情報記憶装置への読み書きが出来る有効な期間が、該端末機能の停止で終了することを特徴とする情報システム。

【請求項８】請求項１において、前記認証情報記憶装置が利用者の操作で前記端末装置から分離して携帯出来ることを特徴とする情報システム。

【請求項９】請求項２において、前記認証情報記憶装置が利用者の操作で前記端末装置から分離して携帯でき、予め第一認証情報によって行った前記認証情報記憶装置への読み書きが出来る有効な期間が、前記認証情報記憶装置を前記端末装置から分離した時に終了することを特徴とする情報システム。

【請求項１０】請求項１において、前記認証情報記憶装置が記憶したデータの読み書きを自由に行うことが可能で、前記端末装置が利用者が暗記する暗証情報を鍵データとしてデータの暗号化と復号化を行う機能を備え、
前記第二認証情報を暗号化して認証情報記憶装置に記憶させ、必要に応じて前記暗証情報によって前記記憶させた暗号情報を復号化して第二認証情報を読み出すようにし、第二認証情報が漏洩するのを防止すると共に、唯一前記暗証情報だけを覚えるだけで簡単な選択で必要な第二認証情報を読み出して、前記ホスト装置への接続に必要な確認処理を完了できるようにしたことを特徴とする情報システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、特定情報あるいは特定ホスト装置に対する利用者認証に係わり、特に利用者認証情報が対象情報毎あるいはホスト装置毎に異なる場合に、利用者がこれら複数の認証情報を覚える必要がない情報システムに関する。

【０００２】

【従来の技術】近年、インターネット上で急速に広がっているWorld Wide Web（欧州核物理学研究所で開発されたドキュメントシステムで以下、WWW）に代表されるように、ネットワーク上の情報提供システム（例えばWWWサーバ）では特定のホスト装置への接続のみならず、そのホスト装置の認証が終了した後も、さらにその中にある特定の情報に対しても利用者の認証を求められる場合がある。

【０００３】この場合、利用者はその都度予め取得した認証情報をホスト装置に送信する必要がある。

【０００４】

【発明が解決しようとする課題】しかしながらこれら認証情報は、ホスト装置の管理者の都合で決定されたものを利用する場合があり、このような時は認証情報がホスト装置毎または情報毎に異なるのが通例である。しかし、これでは利用者は必要な認証情報をすべて覚えている必要があり、非常に煩わしい。

【０００５】しかも、認証情報は利用者本人以外へ漏れることが無いように扱う必要があるので、メモ書き等を残すことは好ましくない。

【０００６】本発明の目的は上記の点に鑑みてなされたもので、その目的は、利用者は唯一、一個の認証情報を入力するだけで、その後はホスト装置または情報への認証処理が簡単に行えるようにすることにある。

【０００７】

【課題を解決するための手段】上記目的を達成する本発明の要旨は、ホスト装置へ送信する複数の認証情報を記憶し、またこの認証情報を読み出す為に送信するものとは別に認証情報を必要とし、さらにこの別に用意した認証情報を確認するための機能を有する認証情報記憶装置と、認証情報記憶装置への認証情報の書き込み、あるいは同装置から認証情報を読み出す機能を有する端末装置を備える。

【０００８】

【発明の実施の形態】以下、本発明の詳細を図示した各実施例によって説明する。

【０００９】〔第一実施例〕図１は、本発明の第一実施例に係わる情報システムの概念図である。本実施例は、プロトコルを使い、インターネット４上のWWWサーバから利用者１０が必要とする情報を取り寄せる例を示したものである。

【００１０】図１において、１，２および３は情報を蓄積しインターネット４に接続されたWWWに対応したホスト装置Ａ，ＢおよびＣで、これらは後述する端末装置８と接続するときに、利用者１０が正規の利用者であることを確認するために、第二認証情報を要求する。４はホスト装置間または利用者１０との間で情報の送受信を可能にするネットワークでインターネット、５は利用者１０とインターネット４の仲介を契約によって行うインターネットプロバイダである。また、６は利用者１０とインターネットプロバイダ５を接続する公衆回線網、７は公衆回線網６から端末装置８までを接続する公衆回線。

【００１１】８は利用者１０がWWWから情報を取り出すために使用する端末装置で、後述するWWWを利用するためのブラウザソフト１２を搭載しており、情報の表示と利用者からの入力が出来る機能を持ち、さらに後述する認証情報記憶装置９に記憶されたデータの読み書きが可能である。９は端末装置８をホスト装置に接続するために要求される第二認証情報と、この第二認証情報が他に漏れないように保護するための第一認証情報を記憶し、また端末装置８で第二認証情報の読み書きを行う時は、必ず第一認証情報により予め認証処理を行う機能を内蔵しており、さらに図５で後述する検索条件により第二認証情報を選択的に読み書きする機能も備えた認証情報記憶装置である。

【００１２】１０は本システムの利用者、１１はホスト装置と端末装置８の間のインターネット４および公衆回線７上で、情報のデータを乗せて流れるプロトコルのパケットである。

【００１３】１２はプロトコルによってホスト装置と通信を行い、ホスト装置に格納された文書を端末装置８の表示機能により利用者１０に提示するソフトウェアでブラウザソフトである。ブラウザソフト１２は利用者１０から入力されたホスト装置や文書名を表わす情報に基づいてインターネット４にアクセスし、ホスト装置より認証情報が要求されたことを検出して、認証情報を認証情報記憶手段９より読み出して送信する機能と、未だ第一認証情報の認証が完了していないために第二認証情報を読み出せない場合には、第一認証情報の入力を利用者１０に要求する機能を備える。

【００１４】図２は本実施例においてホスト装置Ａ１、ホスト装置Ｂ２およびホスト装置Ｃ３から情報を取得するために必要となる「利用者ＩＤ」とそれぞれに対応した「認証情報」、および各ホストを表わす「サーバ名」の例を示している。ここでは、ホスト装置Ｂ２とホスト装置Ｃ３の認証情報は同じであるが、それ以外は全て異なるものが必要であり、これらを一通り覚えるのは面倒である。

【００１５】図３は本実施例において、ブラウザソフト１２が利用者１０に対して認証情報記憶装置９の読み書きを可能にするための第一認証情報を要求している様子を示しており、８１はその第一認証情報を入力する認証情報入力欄である。

【００１６】図４は本実施例において、利用者１０が端末装置８をホスト装置Ａ１に接続したときの端末装置８の画面の例で、８２はインターネット４上で特定のホスト装置を指定するための記述手段であるUnifom Resource Locator（以下ＵＲＬ）であり、“//www.earth.co.jp”はサーバ名で、“／pubindex.htm”はホスト装置から取り寄せる文書名を表わしている。

【００１７】本実施例では、この“pubindex.htm”という文書の取得に認証情報が要求されるとする。また、８３は前述の文書を参照するために必要な利用者名を入力する利用者ＩＤ入力欄で、８４は同じく第二認証情報を入力するための認証情報入力欄である。

【００１８】図５は本実施例において、認証情報記憶装置９の中に各認証情報を記憶するときのデータ構造の例

を示したもので、９１は認証情報記憶装置９の利用者１０を確認するための第一認証情報であり、これが認証されないとこれに続く他のデータへの読み書きが認証情報記憶装置９自身によって禁止される。

【００１９】また９２は図２に示したホスト装置へ送信する第二認証情報で、９３はこの第二認証情報を簡単に選択できるようにするための検索条件であり、本実施例ではサーバ名と文書名を利用している。さらに、９４は利用者ＩＤ、９５は認証情報で、これらは第二認証情報９２の要素データである。なお、認証情報記憶装置９の中で第二認証情報９２と検索条件９３は一組にしてレコードという簡単で扱われ、ブラウザソフト１２によって読み書きされる。

【００２０】図６は本実施例において、ホスト装置Ａ１より文書“pubindex.htm”を端末装置８に取り寄せるときの流れを示した図であり、処理はＳ１からＳ１０へと進む。

【００２１】本実施例の動作を図１～図６を用いて説明する。ここで、利用者１０はすでに図２に示すようにインターネット４上のホスト装置Ａ１、ホスト装置Ｂ２、およびホスト装置Ｃ３を利用するための、第二認証情報９２（利用者ＩＤ９４と認証情報９５）を取得しており、これらの情報は図５に示すように、認証情報記憶装置９に検索条件９３と共に記憶されている。そして、これから利用者１０は公衆回線６を介して、インターネット４に接続されたホスト装置Ａ１から情報を取り寄せようとしているとする。

【００２２】まず、利用者１０は図６に示すように、端末装置８を起動（Ｓ１）し、次で認証情報記憶装置９を端末装置８に接続する（Ｓ２）。

【００２３】次に、利用者１０は図１にあるようにブラウザソフト１２を使って、端末装置８を公衆回線７から公衆回線網６を通してインターネットプロバイダ５に接続し、さらに図４のようにＵＲＬ８２にホスト装置Ａ１のサーバ名“//www.earth.co.jp”を指定して、インターネット４を介してホスト装置Ａ１へ接続を行う（Ｓ３）。そして、目的の文書名“pubindex.htm”をパケット１１に乗せてホスト装置Ａ１へ送信する（Ｓ４）。

【００２４】ここで、ホスト装置Ａ１は文書“pubindex.htm”に認証確認が設定されていると、このことを端末装置８へ通知し、利用者に対して第二認証情報９２の送信を要求する。すると端末装置８のブラウザソフト１２はこの要求を検出（Ｓ５）して、認証情報記憶装置９から検索条件９３を用いて第二認証情報９２の取得を試みる。

【００２５】しかし、本実施例では図６のＳ５までの間に未だ第一認証情報９１の確認が行われていないため、ブラウザソフト１２が認証情報記憶装置９から第二認証情報９２を取り出そうとしても、認証情報記憶装置９によってその操作が拒否されてしまう。そこで、ブラウザソフト１２は図３に示すように、利用者１０に対して第一認証情報９１の入力を促す（Ｓ６）。

【００２６】利用者１０が認証情報入力欄８１に第一認証情報９１“Treasure Box”を入力し、「ＯＫ」を指示すると、ブラウザソフト１２は端末装置８を介して第一認証情報９１を認証情報記憶装置９に入力する。第一認証情報９１を受け取った認証情報記憶装置９は、これと記憶している第一認証情報が一致するかどうかを確認し、一致した場合には、第二認証情報９２の取り出しを許可する（Ｓ７）。

【００２７】もし、一致しなかった場合には利用者１０に対し警告するメッセージの表示や、再入力を促すように動作する。

【００２８】Ｓ７において確認がされると、次にブラウザソフト１２は認証情報記憶装置９に第二認証情報９２を検索させるためにＵＲＬ８２に含まれているサーバ名および文書名を渡す。サーバ名と文書名を受け取った認証情報記憶装置９は、図５に示すようにレコード単位で記憶されたデータから検索条件９３を順次取り出し、これとサーバ名および文書名を比較して、一致するレコードを探す。

【００２９】本実施例では図５で先頭にあるレコードが検索条件９３を満たすので、認証情報記憶装置９は同じレコードから検索条件９３に続いて記憶されている第二認証情報９２（利用者ＩＤ９４“IslandＡＢＣ”および認証情報９５“１７３１６１ｎ６４”）を取り出し、これをブラウザソフト１２に渡す（Ｓ８）。

【００３０】ブラウザソフト１２はこのようにして第二認証情報９２を受け取ると、図４に示した利用者ＩＤ入力欄８３と、認証情報入力欄８４からホスト装置Ａ１に対して第二認証情報９２を送信する。第二認証情報９２を受信したホスト装置Ａ１は、これを文書“pubindex.htm”に設定されている認証情報と比較し、一致が確認（Ｓ９）できると、文書“pubindex.htm”をパケット１１に乗せて送信を開始し、ブラウザソフト１２はパケット１１を順次受信して、端末装置８の画面に文書を表示する（Ｓ１０）。

【００３１】以降、利用者１０が新たなＵＲＬ８２を入力し、第二認証情報９２が要求される度に、図６に示すＳ４からＳ１０の処理を繰り返すが、第一認証情報９１の確認は既に完了しているので、Ｓ６およびＳ７はスキップされる。

【００３２】なお、図６の流れ図では示していないが、もしもＳ８で検索条件９３と一致するレコードが記憶されていないときには、要求された第二認証情報９２が記憶されていないことを利用者１０に通知する表示と共に、図４の表示で利用者ＩＤ入力欄８３と認証情報入力欄８４が共に空白の表示を行い、そして、ここでもし利用者１０が検索条件９３に対応する第二認証情報９２を

入力すれば、この認証情報は新規の第二認証情報として認証情報記憶装置９に検索条件９３と共に記憶され、次回同じ検索条件９３でレコードの検索が行われたときには、自動的に第二認証情報の読み出し処理が行われるようになる。

【００３３】また、図５で検索条件９３が“ｗｗｗ．ｗｏｒｌｄ-ｗｉｄｅ．ｃｏ．ｊｐ”のレコードには利用者ＩＤ“Ｇｕｅｓｔ”だけが記憶されているが、これはこのホスト装置が認証情報９５を必要としないからである。

【００３４】このように処理が行われることにより利用者１０は、一度だけ認証情報記憶装置９を利用するための第一認証情報９１を入力しておけば、特定のホスト装置あるいは特定の文書毎に第二認証情報を要求されるような場合、さらにはそのような認証情報の内容がばらばらであるような場合でも、必要とされる第二認証情報が予め認証情報記憶装置９に記憶してあれば、利用者１０が暗記している第二認証情報９２を毎回手動で図４の利用者ＩＤ入力欄８３と認証情報入力欄８４に入力しなくても、自動的に第二認証情報９２が送信されるので、入力の間違いがなくなるだけでなく、複数ある認証情報をまとめて一個の認証情報を覚えておくだけで利用できるので非常に使い勝手が良い。

【００３５】また、認証情報は利用者以外に漏れることがないようにしなければならないが、本実施例では認証情報記憶装置９自身に記憶したデータの読書きを制限する機能を備えているので、たとえ端末装置８から分離して紛失したような場合でも、第二認証情報９２が他人に漏れる心配が無い。もちろん、認証情報記憶装置９が端末装置８と一体になっているような場合でもこれらの利点が失われることがないのは明白である。

【００３６】さらに、実施例では説明しなかったが、図６でＳ２を行わなかったときは、端末装置８をホスト装置Ａ１に接続し、文書“ｐｕｂｉｎｄｅｘ．ｈｔｍ”を指定したときに、認証情報記憶装置９が端末装置８に接続されていないことをブラウザソフト１２が検出し、利用者１０に対して認証情報記憶装置９を端末装置８に接続することを促すメッセージを表示する。そして表示にしたがって、利用者１０が認証情報記憶装置９を端末装置８に接続すると、図３に示したように、第一認証情報９１を入力する画面を表示するようにもできる。

【００３７】また、本実施例では検索条件９３としてＵＲＬ８２に含まれるサーバ名や文書名を利用するようにしたが、検索条件にはこれら以外にもホスト装置と端末装置間のデータ送受信を行っているプロトコルに含まれるデータ、例えばＩＰアドレスも使うことが可能であり、文書名もそのホスト装置が認証を設定可能なテキスト、音声、画像、などファイルさまざまなものが利用できることは容易に想像できる。

【００３８】なお、本実施例では第一認証情報が確認されていれば、後は自動的に第二認証情報が読み出されるようにしたが、もちろん第二認証情報が必要になる毎に第一認証情報の入力を利用者に要求することも可能で、この場合利用者は多少の不便を被るが、第一認証情報が確認済みの状態で端末装置を放置してしまうと、第三者でも容易にホスト装置の利用が可能になるので、これを防止するためには役立つ。

【００３９】図７は上記に関して、別の実現形態を示すもので、第一認証情報９１の確認が完了した後の認証情報記憶装置９への読み書きが出来る有効な期間を終了させる方式の例を示したものである。図７では、認証情報記憶装置９が端末装置８と分離可能である場合を想定し、４種類の条件で上記の有効期間を終了する。

【００４０】まず、認証情報記憶装置９の読書き有効期間が開始すると、端末装置８またはブラウザソフト１２は定期的に図７の流れで、（１）端末装置８とホスト装置との接続終了、（２）予め端末装置８かブラウザソフト１２に設定されている期間端末装置８が放置された、（３）認証情報記憶装置９の中に独立して設定された期間が経過した、（４）認証情報記憶装置９が端末装置８から分離された、と云う以上の条件を順次確認し、いずれかに該当したときに認証情報の読書き有効期間を終了させ、再び第二認証情報９２が必要なときは第一認証情報の確認からやり直すようにしたものである。もちろん、条件としてこれ以外にも、電源電圧が低下した場合や、認証情報記憶装置９が分離されなくても利用者の手が触れた場合などが考えられる。

【００４１】さらに、本実施例では認証情報記憶装置９の読み書きは同時に一つの認証情報で許可されるようにしたが、例えば認証情報記憶装置９の読取りと、書き込みを異なる認証情報で出来るようにすれば、ホスト装置を管理している管理者が、まず書き込み用の認証情報で必要な第二認証情報を記憶し、その後この認証情報記憶装置９を利用者に配布することによって、利用者に対してホスト装置への接続を制限する一方で、利用者毎に一個の第二認証情報だけでホスト装置（複数も含む）を管理出来ない場合でも、利用者は読み出し用の第一認証情報だけを覚えるだけで戸惑うことなくホスト装置を利用できる。もちろん、読み出し用の第一認証情報はその利用者のみが知っているものなので、セキュリティも保つことが出来る。

【００４２】なお、本実施例では特に図示しないが、認証情報記憶装置９へ第二認証情報９２を記憶させる手順は、読み出しと同様にまず第一認証情報９１を入力して、次いで検索条件９３とこれに対応する第二認証情報９２を書き込むことで行えるが、既に記憶しているレコードに書き込もうとした検索条件９３と完全に一致する検索条件がある場合には、第二認証情報の更新をする旨を利用者１０に通知する。さらに、認証情報記憶装置９に記憶できる空き領域が不足した場合には、新しい認証情報記憶装置９を用意することを利用者１０に促すが、

新しい認証情報記憶装置９に交換したときには、始めに第一認証情報の設定を行い、その後第二認証情報を書き込むことになる。

【００４３】また図８は図５のデータ構造において、各レコード毎に第二認証情報９２に関する属性情報９６を付加した例で、属性情報９６には例えば各第二認証情報の使用回数や、何に関するホスト装置であるか、あるいはその認証情報をいつ取得したか、さらにその第二認証情報９２の有効期限などを記録しておくことで、認証情報の削除や更新などのメンテナンスに利用することが出来る。

【００４４】なお、以上に説明した本実施例に利用できる認証情報記憶装置の形状や接続方式は、分離型で携帯性を重視するような場合には、例えばＩＳＯ７８１６に準拠したＩＣカードが挙げられる。

【００４５】また端末装置に内蔵するような場合は、同じくＩＳＯ７８１６に準拠する機能をもったＩＣチップを実装するか、またはこのような機能を端末装置を制御するＣＰＵと一緒に一つのＩＣチップに収めるなどが考えられる。

【００４６】〔第二実施例〕図９は、本発明の第二実施例に係わる情報システムの概念図である。本実施例は、認証情報を記憶する装置として、記憶したデータの読み書きに関して何ら保護する機能を持たないものを使用した場合の例である。ただし、第一実施例と同様に複数の第二認証情報９２を記憶し、利用者１０はこれらを一個の情報を覚えるだけで必要に応じてホスト装置へ送信することが出来るようにしている点は同じである。また、同図において、先の実施例と均等なものには同一番号を付し、その説明は重複を避ける為に省略する。

【００４７】図９において、１３は端末装置８をホスト装置に接続するために要求される情報を記憶するが、データの読み書きは認証情報などの制約無しにいつでも行えるデータ記憶装置である。

【００４８】１４はデータ記憶装置１３に記憶する第二認証情報９２を後述する暗証情報１６によって暗号化して暗号第二認証情報９７を出力する第二認証情報暗号化処理、１５は第二認証情報暗号化処理１４とは逆に、暗証情報１６で暗号第二認証情報９７を復号化して元の第二認証情報９２を出力する第二認証情報復号化処理、１６は利用者１０が暗記している情報で、第二認証情報暗号化処理１４および第二認証情報復号化処理１５において第二認証情報９２を暗号化および復号化する際の鍵情報となる暗証情報である。９７は第二認証情報暗号化処理１４で暗証情報１６によって暗号化された第二認証情報で、データ記憶装置１３に記憶されている暗号第二認証情報である。

【００４９】図１０は本実施例において、ホスト装置Ａ１より文書“pubindex.htm”を端末装置８に取り寄せるときの流れを示した図であり、処理はＳ１からＳ１０へと進む。

【００５０】本実施例の動作を図９および図１０を用いて説明する。

【００５１】ここでは、第一実施例と同様にホスト装置Ａ１に目的の情報があり、ホスト装置Ａ１はインターネット４に接続されており、目的の情報はＵＲＬ８２で指定し、さらに指定された情報は第二認証情報が要求されるとする。

【００５２】まず、利用者１０は図１０に示すように、まず端末装置８を起動（Ｓ１）し、データ記憶装置１３を端末装置８に接続する（Ｓ２）。

【００５３】次に、利用者１０は図９にあるようにブラウザソフト１２を使って、端末装置８を公衆回線７から公衆回線網６を通じてインターネットプロバイダ５に接続し、ＵＲＬ８２を指定してホスト装置Ａ１に接続を行い（Ｓ３）、そして目的の文書名“pubindex.htm”をパケット１１に乗せてホスト装置Ａ１へ送信（Ｓ４）。ホスト装置Ａ１は文書“pubindex.htm”に認証確認が設定されていると、この事を端末装置８へ通知し、利用者１０に対して第二認証情報９２の送信を要求する。ここまでは第一実施例と同様である。

【００５４】次に、第二認証情報９２の送信を要求された端末装置８のブラウザソフト１２はこの要求を検出（Ｓ５）すると、ＵＲＬ８２から検索条件９３を取り出し、データ記憶装置１３から検索条件９３を用いて暗号第二認証情報９７を読み出す（Ｓ６）。

【００５５】読み出された暗号第二認証情報９７は暗号化された状態なので、復号化の必要がある。そこでブラウザソフト１２は利用者１０に暗証情報１６の入力を要求する（Ｓ７）。

【００５６】暗証情報１６を入力されると、ブラウザソフト１２はこれを第二認証情報復号化処理１５に暗号第二認証情報９７と共に入力し、復号化し第二認証情報９２を得る。

【００５７】ブラウザソフト１２はこのようにして第二認証情報９２を受け取ると、第一実施例と同様に図４に示した利用者ＩＤ入力欄８３と、認証情報入力欄８４からホスト装置Ａ１に対して第二認証情報９２を送信し、これが確認（Ｓ９）されると、文書“pubindex.htm”が送信され、ブラウザソフト１２はこれを順次受信して、端末装置８の画面に文書を表示する（Ｓ１０）。

【００５８】以降、利用者１０が新たなＵＲＬ８２を入力し、第二認証情報９２が要求される度に、図１０に示すＳ４からＳ１０の処理を繰り返すが、暗証情報１６は一度入力したので、Ｓ７はスキップされる。

【００５９】このように処理が行われることにより利用者１０は、一度だけ暗証情報１６を入力しておけば、特定のホスト装置あるいは特定の文書毎に第二認証情報を要求されるような場合、さらにはそのような認証情報の内容がばらばらであるような場合でも、必要とされる第

二認証情報が予めデータ記憶装置１３に記憶してあれば、自動的に第二認証情報９２が送信されるので、複数ある認証情報をまとめて一個の暗証情報を覚えておくだけで利用できるので非常に使い勝手が良い。

【００６０】また、認証情報は利用者以外に漏れることがないようにしなければならないが、本実施例ではデータ記憶装置１３に記憶されたデータは暗号化されているので、たとえ端末装置８から分離して紛失したような場合でも、第二認証情報９２が他人に漏れる心配が無い。もちろん、データ記憶装置１３が端末装置８と一体になっているような場合でもこれらの利点が失われることがないのは明白である。

【００６１】なお、以上のように構成することで、第一実施例で説明した第二認証情報を自動的に読み出せる有効期限の制御や、検索条件に該当するものがないときの処理、同じ検索条件での第二認証情報は更新処理を実行、属性情報の付加、データ記憶装置が端末装置に接続されていないときの処理、検索条件を構成するデータの種類などは第一実施例と同等のものを本実施例でも実現できる。

【００６２】また、本実施例のようにデータ記憶装置自身には記憶した情報を保護する機能がなく、そのため記憶するデータ自身を暗号化するなどして漏洩を防止した場合、端末装置の仕様またはブラウザソフトの機能が同じであれば、データ記憶装置を単体で持ち歩き、他の端末装置からでもホスト装置を利用できるが、データ記憶装置内のデータ記録フォーマットの違いや、暗号化／復号化処理の有無あるいは相違があると、利用できない。

【００６３】そこでこれらへの対応には、例えば記録フォーマットでは、同じデータを複数の形式のフォーマットで記憶することで改善できる。また、暗号化や復号化の処理はこれらの処理を行うプログラムをその端末のアーキテクチャに合わせて作り、これまた複数の形式のフォーマットで記憶しておくことで改善を図れる。

【００６４】

【発明の効果】本発明によれば、利用者は情報をホスト装置から取寄せる時に、複数の認証情報をホスト装置に送信する必要がある場合でも、利用者は唯一、一個の認証情報を入力するだけで、その後はホスト装置または情報への認証処理が簡単に行えるようになる。

【図面の簡単な説明】

【図１】第一実施例の情報システムの概念図である。

【図２】第一実施例および第二実施例を説明するためのホスト装置に登録されている利用者ＩＤなどの例を示す図である。

【図３】第一実施例および第二実施例を説明するための画面表示の例を示す図である。

【図４】第一実施例および第二実施例を説明するための画面表示の例を示す図である。

【図５】第一実施例のデータ構造を説明する図である。

【図６】第一実施例の処理の流れを示す説明図である。

【図７】第一実施例で認証情報を自動的に取り出せる期間の制御を説明するフロー図である。

【図８】第一実施例のデータ構造の説明を補足する図である。

【図９】第二実施例である情報システムの概念図である。

【図１０】第二実施例の処理の流れを示す説明図である。

【符号の説明】

１…ホスト装置Ａ、　２…ホスト装置Ｂ、　３…ホスト装置Ｃ、４…インターネット、　５…インターネットプロバイダ、６…公衆回線網、　７…公衆回線、８…端末装置、８１…認証情報入力欄、８２…Uniform Resource Locator(ＵＲＬ)、８３…利用者ＩＤ入力欄、　８４…認証情報入力欄、９…認証情報記憶装置、　９１…第一認証情報、９２…第二認証情報、　９３…検索条件、　９４…利用者ＩＤ、９５…認証情報、９６…属性情報、　９７…暗号第二認証情報、１０…利用者、　１１…パケット、　１２…ブラウザソフト、１３…データ記憶装置、１４…第二認証情報暗号化処理、１５…第二認証情報復号化処理、１６…暗証情報。

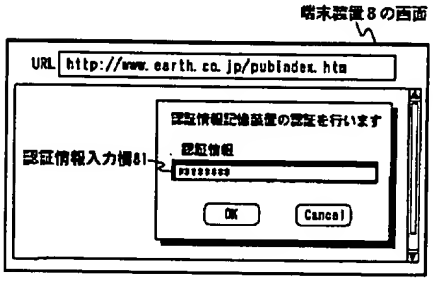
【図２】

図 2

ホスト装置	利用者ＩＤ	認証情報	サーバ名
A	IslandABC	173161n54	//www.earth.co.jp
B	Jungle123	4Au6Eg6Ce	//www.peace.co.jp
C	CanyonXYZ	4Au6Eg6Ce	//www.space.co.jp

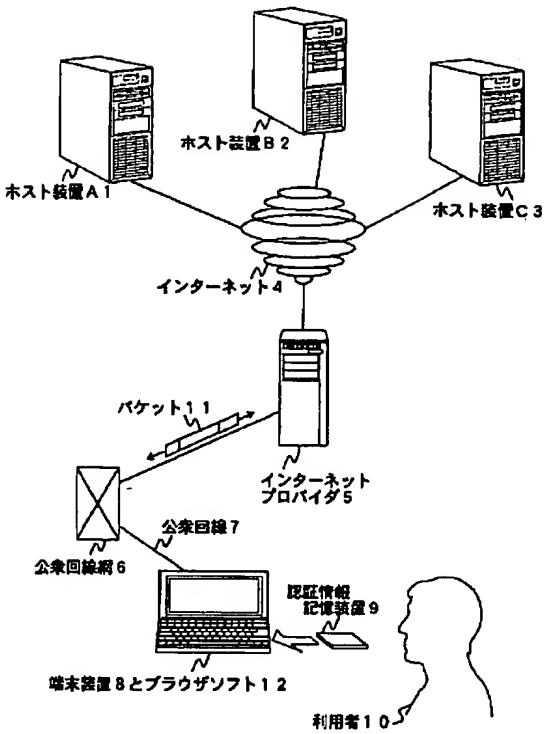
【図３】

図 3



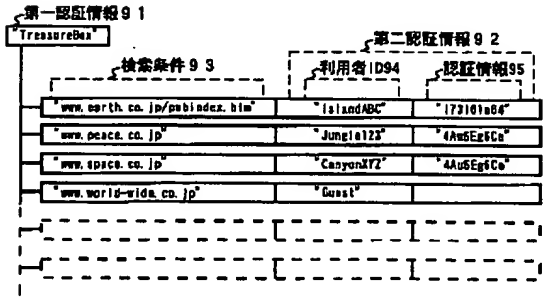
【図１】

図 1



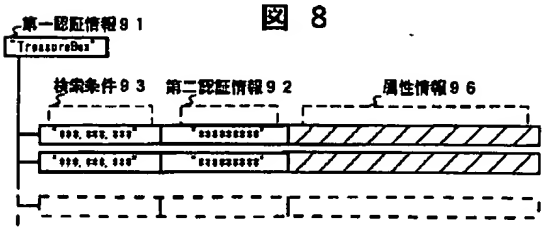
【図５】

図 5



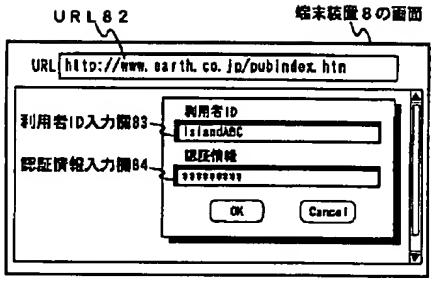
【図８】

図 8



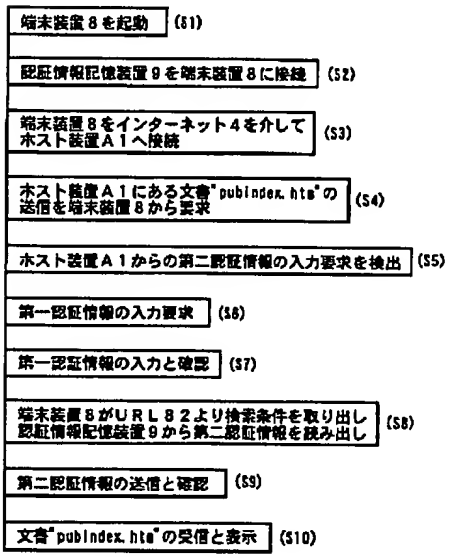
【図４】

図 4



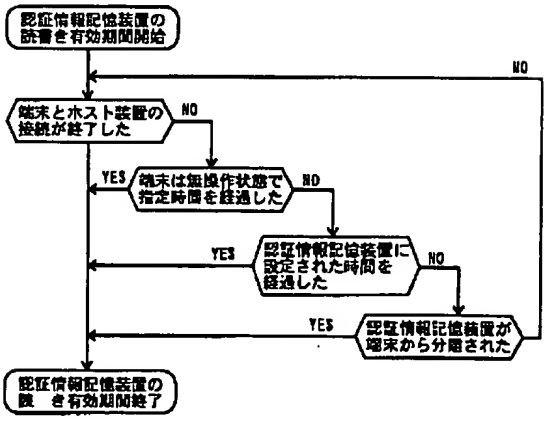
【図６】

図 6



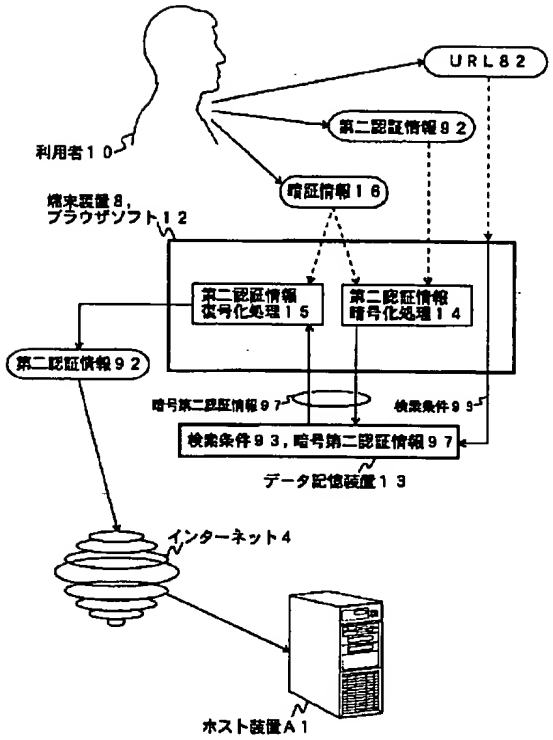
【図７】

図 7



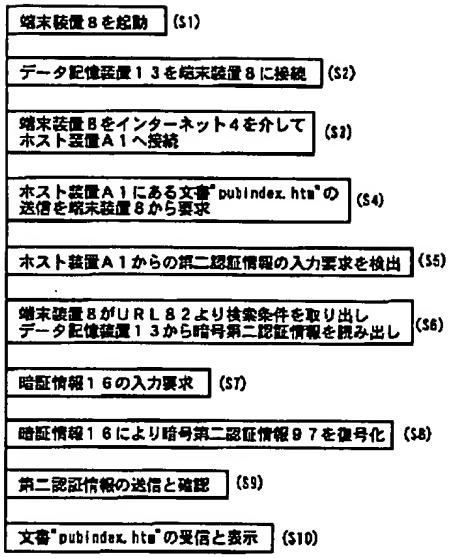
【図９】

図 9


利用者１０
ＵＲＬ８２
第二認証情報９２
暗証情報１６
端末装置８，
ブラウザソフト１２
第二認証情報
復号化処理１５
第二認証情報
暗号化処理１４
第二認証情報９２
暗号第二認証情報９７
検索条件９９
検索条件９３，暗号第二認証情報９７
データ記憶装置１３
インターネット４
ホスト装置Ａ１

【図１０】

図 10


端末装置８を起動 (S1)
データ記憶装置１３を端末装置８に接続 (S2)
端末装置８をインターネット４を介して
ホスト装置Ａ１へ接続 (S3)
ホスト装置Ａ１にある文書"pubindex.htm"の
送信を端末装置８から要求 (S4)
ホスト装置Ａ１からの第二認証情報の入力要求を検出 (S5)
端末装置８がＵＲＬ８２より検索条件を取り出し
データ記憶装置１３から暗号第二認証情報を読み出し (S6)
暗証情報１６の入力要求 (S7)
暗証情報１６により暗号第二認証情報９７を復号化 (S8)
第二認証情報の送信と確認 (S9)
文書"pubindex.htm"の受信と表示 (S10)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-025051
(43)Date of publication of application : 29.01.1999

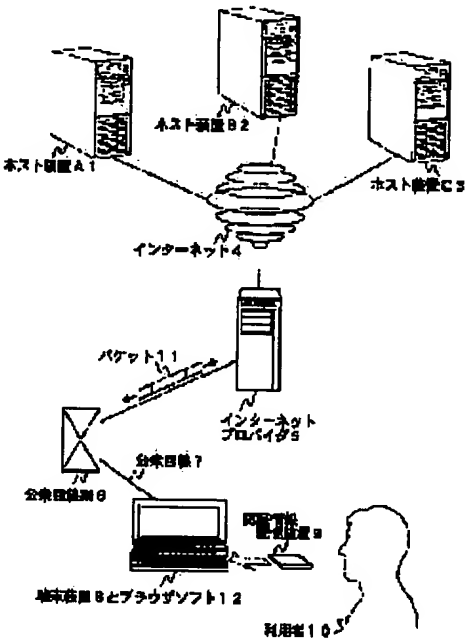
(51)Int.CI. G06F 15/00
G06F 1/00

(21)Application number : 09-183433
(22)Date of filing : 09.07.1997

(71)Applicant : HITACHI LTD
(72)Inventor : YOKOZAWA TATSU
ADACHI MAKOTO

(54) INFORMATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve operability by allowing a user to input only one certification information for easily operating a certification processing for a host device or the information afterwards.
SOLUTION: A certification information storage device 9 stores second certification information requested for connecting a terminal equipment 8 with a host device, and first certification information for protecting the second certification information from being leaked to the others. Host devices A1, B2, and C3 corresponding to a word wide web(WWW) connected with an internet 4 request the second certification information for confirming that a user 10 is a legal user at the time of connection with the terminal equipment 8. The user 10 inputs the first certification information only once so that the second certification information can be automatically transmitted when the second certification information is requested for each specific host device or specific document as long as the necessary second certification information is preliminarily stored in the certification information storage device 9.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Dat of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Prior Art Document 2

[Claim 1]

An information system comprising: a host device and a terminal device;

said host device in which various items of information are stored and said items of information are retrievable by a user with said terminal device, said host device having a function for requesting a user authentification information for confirming that the user is an authorized registrant at the time of the retrieval of said items of information by the user; and

said terminal device, which is capable of transmitting/receiving data by connecting to the host device, having a function for retrieving said various items of information and presenting the information to a user, and a function for receiving an input by a user, said information system further comprising:

an authentification information storage device which stores various kinds of data, the data are being readable/writable by said terminal device, and has a function for storing first authentification information for authorizing reading/writing the data before the data are actually read/written, and a function for performing authorization processing; wherein

said authentification information storage device stores authentification information which is required in said host device as second authentification information, and said authentification information storage device or said terminal device has a function for reading/writing the second authentification information selectively, whereby

even in the case where a plurality of kinds of second authentification information are required, a user does not need necessarily to remember respective authentification information but need to remember said first authentification information, thereby enabling the user to read out necessary second authentification information by easy selection to complete confirmation operation necessary for establishing a connection to said host device.

[Claim 2]

The information system according to claim 1, wherein:

said host device and said terminal device have a function for transmitting/receiving information by protocol, respectively; and

said terminal device has a function for detecting, by the protocol, whether or not confirmation operation is necessary for connecting to said host device, a function for reading out said second authentification information from said authentification information storage device and transmitting it to said host device in response to the success of detection and a function for performing the confirmation operation in advance with regard to said authentification information storage device using said first authentification information; whereby

a user does not need necessarily to input said first authentification information, every time the user is requested, by said host device, to input said second authentification information.

[0014]

Fig. 2 shows examples of "user ID", its corresponding "authentication information" required to obtain information from a host device A1, a host device B2, and a host device C3, and "server name" indicating the respective host device.

【Fig. 2】

HOST DEVICE	USER ID	AUTHENTICATION INFORMATION	SERVER NAME
A	IslandABC	173161n64	//www.earth.co.jp
B	Jungle123	4Au6Eg6Ce	//www.peace.co.jp
C	CanyonXYZ	4Au6Eg6Ce	//www.space.co.jp